ON THE NON-TRIVIALITY OF $G(D)$ AND THE EXISTENCE OF MAXIMAL SUBGROUPS OF $GL_1(D)$

T. KESHAVARZIPOUR & M. MAHDAVI-HEZAVEHI

Abstract. Let D be an F-central division algebra of index n. Here we investigate a conjecture posed in [4] that if D is not a quaternion algebra, then the group $G_0(D) = D^*/F^*D'$ is non-trivial. Assume that either D is cyclic or F contains a primitive p-th root of unity for some prime $p|n$. Using Merkurjev-Suslin Theorem, it is essentially shown that if none of the primary components of D is a quaternion algebra, then $G(D) = D^*/RN_{D/F}(D^*)D' \neq 1$. In this direction, we also study a conjecture posed in [1] or also [7] on the existence of maximal subgroups of D^*. It is shown that if D is not a quaternion algebra with $i(D) = p^e$, then D^* has a maximal subgroup if either of the following conditions holds: (i) F has characteristic zero, or (ii) F has characteristic p, or (iii) F contains a primitive p-th root of unity.

Let D be an F-central division algebra of index n. Denote by D' the commutator subgroup of the multiplicative group D^*. Given a subgroup G of D^*, we shall say that G is *maximal* in D^* if for any subgroup H of D^* with $G \subset H$, one concludes that $H = D^*$. We know, by Corollary 1 of [8], that $G(D) := D^*/RN(D^*)D'$, where $RN(D^*)$ is the image of D^* under the reduced norm of D to F, is an abelian torsion group of a bounded exponent dividing the index of D over F. This group is not trivial in general. For instance, if D is the algebra of real quaternions, then $G(D)$ is trivial whereas for rational quaternions $G(D)$ is isomorphic to a direct product of copies of Z_2, as it is easily checked. Assume that $G(D)$ is not trivial, then by Prũfer-Baer Theorem (cf. [14], p. 105), we conclude that $G(D)$ is isomorphic to a direct product of Z_{r_i}, where r_i divides the index of D over F. In this way, one may obtain normal maximal subgroups of finite index in D^*. So, if $G(D)$ is not trivial, then D^* contains maximal subgroups. For some examples of non-normal maximal subgroups of D^*, see [9]. It is shown in [9] that even for the case $G(D) = 1$, we may obtain maximal subgroups in D^*. But, the question of whether D^* contains

1991 *Mathematics Subject Classification.* 16K20.

Key words and phrases. division ring, maximal subgroup, splitting field.

a maximal subgroup for any noncommutative division ring D, is still open. In this note, we concentrate on the case where D is of finite dimension over its centre such that $G(D)$ is trivial. When $i(D) = p^e$, p a prime, and $G(D) = 1$, it is shown in Theorem 1 and Theorem 3 that if either D is an F-central cyclic division algebra or F contains a primitive p-th root of unity, then D is a quaternion algebra. Also, in Proposition 1, it is proved that if one of the primary components of D is a p-algebra for some prime $p|n$, then $G(D) \neq 1$. We then proceed to explore suitable conditions on D such that D^* contains a maximal subgroup for an arbitrary division algebra of index n. It is essentially shown that when D is not a quaternion algebra with $i(D) = p^e$, then D^* contains a maximal subgroup if either of the following conditions holds: (i) F has characteristic zero, or (ii) F has characteristic p, or (iii) F has a primitive p-th root of unity. We shall use the conventions and notations of [2] throughout. We begin our study with the following:

Lemma 1. *Let A be an F-central cyclic algebra of odd index n such that the skew field component of A is noncommutative. Then $G_0(A) := A^*/F^*A' \neq 1$, where A' is the commutator subgroup of A^*.*

Proof. We know that $A \simeq \oplus_{i=0}^{n-1} Ka^i$, where K/F is cyclic of degree n with $a^n = \alpha \in F$. Thus, a is a root of the minimal polynomial $x^n - \alpha$. Now, we have $RN_{A/F}(a) = (-1)^{n+1}\alpha$. Assume on the contrary that $G_0(A) = 1$. Then there exist $f \in F^*$ and $c \in A'$ such that $a = fc$. Hence, $RN_{A/F}(a) = f^n$ and therefore, $f^n = (-1)^{n+1}\alpha$. Since n is odd, we obtain $f^n = \alpha$ and hence $\alpha \in N_{K/F}(K^*)$. But this, by Theorem 14.7 of [6], contradicts the assumption $A \not\simeq M_r(F)$ for any r, and so the result follows. □

The next result deals with F-central cyclic division algebras of degree a power of 2 such that $G_0(D)$ is trivial. It is shown that in this case our cyclic division algebra takes a particular simple form.

Lemma 2. *Let D be an F-central cyclic division algebra of index $n = 2^m$ such that $G_0(D) = 1$. Then we have the following:*

(i) *There is an element $a \in D^*$ and a maximal subfield K such that $D \simeq \oplus_{i=0}^{n-1} Ka^i$ with $a^n = -1$; where K/F is cyclic, $Gal(K/F) =< \sigma >$, and $ax = \sigma(x)a$, for all $x \in K$.*

(ii) *The left K-space D_1 generated by even powers of a, i.e., $D_1 := \oplus_{i=0}^{n/2-1} Ka^{2i}$ is a cyclic division algebra with maximal subfield K and center E such that $[E : F] = 2$.*

Furthermore, (i) is valid for any F-central cyclic algebra A with index $n = 2^m$ and $G_0(A) = 1$.

Proof. (i) Since D is cyclic we have the representation $D \simeq \oplus_{i=0}^{n-1} Ka^i$ for some $a \in D^*$ with $a^n = \alpha \in F$. To end the proof, we claim that it is possible to take $\alpha = -1$. It is clearly seen that a is a root of the minimal polynomial $x^n - \alpha$. Therefore, $RN_{D/F}(a) = (-1)^{n+1}\alpha$. Since $G_0(D) = 1$ we have $a = fc$ for some $f \in F^*$ and $c \in D'$. Thus $RN_{D/F}(a) = f^n$ and hence $f^n = (-1)^{n+1}\alpha$. Since n is even we conclude that $f^n = -\alpha$ and so $a^n = -f^n$, i.e, $(af^{-1})^n = -1$. Therefore, we may replace a by af^{-1} to obtain the result.
(ii) It is easily seen that the left K-space D_1 is closed under addition and multiplication and so D_1 is a ring. We claim that D_1 is a division algebra. To see this, let $x \in D_1$. Then x^{-1} as an element of D, has the form $x^{-1} = y + z$ where $y \in D_1$ and the powers of a occurring in z are all odd. Therefore, $xx^{-1} = x(y+z) = xy + xz = 1$. Since $xz = 1 - xy \in D_1$, and the powers of a occurring in xz are odd, we conclude that $xz = 0$. i.e., $x^{-1} \in D_1$ and the claim is established. It is now clear that K is a maximal subfield of D_1. For dimensional reasons we conclude that $Z(D_1) = E \subset K$ such that $[E : F] = 2$. Therefore, we obtain $D_1 \simeq (-1, K/E, \sigma^2)$. Note that our Galois group here is $\Gamma = \{\sigma^2, \sigma^4, \cdots\}$. □

In the next lemma, we show that for any F-central cyclic division algebra D of index a power of 2, the condition $G_0(D) = 1$ implies that D is a quaternion algebra.

Lemma 3. *Let D be an F-central cyclic division algebra of index $n = 2^m$. If $G_0(D) = 1$, then D is a quaternion algebra.*

Proof. By Lemma 2, we may assume that $D \simeq \oplus_{i=0}^{n-1} Ka^i$ with $a^n = -1$, where K/F is cyclic of degree n and for all $x \in K$, $ax = \sigma(x)a$ with $Gal(K/F) =< \sigma >$. Thus, the characteristic of F is different from 2. Let D_1 be the division subalgebra generated by the even powers of a. By Lemma 2, D_1 is a cyclic division algebra with center E such that $[E : F] = 2$. It is clear that we have $D = D_1 \oplus D_1 a$. If D_1 is commutative, then we obtain $Z(D_1) = D_1 = K = E$ and so $m = 1$, which means that D is a quaternion division algebra. We now claim that $D_1 = E$. i.e., $n > 2$ leads to a contradiction. To see this, set $k = n/2 \neq 1$. Therefore, $a^k \in D_1 \setminus E$, and so E and consequently F contains no square root of -1. Now, since $G_0(D) = 1$, for any $x \in D^*$ we have $x = fc$, for some $f \in F^*$ and $c \in D'$. By Skolem-Noether Theorem, we know that σ is inner. Thus, $\sigma(x) = f\sigma(c) = fdcd^{-1}$ for some $d \in D^*$. Hence, $x\sigma(x) \in F^{*2}D'$ for all $x \in K^*$. Since $CharF \neq 2$ and E/F is Galois of degree 2, we have $N_{E/F}(-1) = 1$. Therefore, by Hilbert's "Satz90", there is an element $b \in E$ such that $b\sigma|_E(b)^{-1} = -1$, where $\sigma|_E$ is the restriction of σ to E. We also have $b\sigma(b) \in F^{*2}D'$. Hence $b^2 \in -F^{*2}D'$, i.e., there is an element $c \in D'$ and $a_1 \in F^*$ such that $b^2 = -a_1^2 c$. This implies that $-a_1^{-2}b^2 = c \in Z(D') = F^* \cap D'$ since $b^2 \in F^*$. Now, since F contains no square root of -1 and, by a result of [11], $Z(D')$ is a finite group of order dividing $i(D) = 2^m$, we conclude that $Z(D') = \{-1, 1\}$. Therefore, we have either $c = 1$ or $c = -1$. If $c = -1$, then $b^2 = a_1^2$ and so $b \in F$. Now, from $b\sigma(b)^{-1} = -1$ we conclude that $charF = 2$ which is a contradiction. Thus, $c = 1$ and we obtain $b^2 = -a_1^2$, i.e., $(ba_1^{-1})^2 = -1$. This implies that E has a square root of -1, that is a contradiction. So we have $k = 1$, i.e, $D_1 = K = E$ and so the result follows. □

We are now able to prove one of our main results in the form of

Theorem 1. *Let D be an F-central cyclic division algebra such that $G_0(D) = 1$, then D is a quaternion algebra.*

Proof. By Corollary 15.3 of [13], we know that a central division algebra is cyclic if and only if its primary components are cyclic. Thus, if $D \simeq \otimes_{i=1}^{k} D_i$ is the primary decomposition of D, then D_i is cyclic division algebra for each i. Now, by a result of [3], we know that $G_0(D) \simeq G_0(D_1) \times \cdots \times G_0(D_k)$. Hence, $G_0(D_i) = 1$ for all $1 \leq i \leq k$. Finally, use Lemma 1 and Lemma 3 to obtain the result. □

To prove our next theorem we shall need the following:

Lemma 4. *Let D be an F-central p-division algebra of index p^e, p a prime. Then D has a cyclic splitting field of degree p^{te}, for some positive integer t.*

Proof. By Theorem 15.4 of [2], there are cyclic extensions $L_1, \ldots, L_r$ of degrees p^{e_i} over F and also elements $a_1, \ldots, a_r \in F^*$ such that $[D] = \Sigma_{i=1}^{r}[a_i, L_i/F, \sigma_i]$, where $Gal(L_i/F) =< \sigma_i >$. Set $A_i := (a_i, L_i/F, \sigma_i)$. By Theorem 4.5.1 of [5], since the tensor product of A_i's is also a cyclic p-algebra, we have $\otimes_{i=1}^{r}(a_i, L_i/F, \sigma_i) = (a, L/F, \sigma)$ for some cyclic extension L/F. Hence, $[L : F] = p^s$ for some integer s. Therefore, L is a cyclic splitting field for D of degree a power of p. Now, by a repeated use of Lemma 15.2 of [2], L can be chosen as a cyclic splitting field for D of degree p^{te} for some positive integer t. □

The next result essentially says that the multiplicative group of every F-central division p-algebra contains a normal maximal subgroup.

Theorem 2. *Let D be an F-central division p-algebra of index p^e. Then we have $G(D) \neq 1$.*

Proof. Assume on the contrary that $G(D) = 1$. By Lemma 4, we may choose a cyclic splitting field E for D such that $[E : F] = p^{te}$ for some integer t. By Theorem 9.7 of [2], we can find an F-central cyclic algebra A such that E is a maximal subfield in A and also $[A] = [D]$. Consequently, $A = M_m(D)$, where $m = p^{(t-1)e}$. Now, we claim that $G(A) = 1$. To prove this, by a theorem in [10], we know that $G(A) = D^*/RN(D)^m D'$. Now, since $G(D) = 1$ we have $D^* = RN(D^*)D'$. By taking reduced norm of both sides of the last relation we obtain $RN(D^*) = RN(D^*)^{p^e}$ and hence $RN(D^*) = RN(D^*)^m$, i.e., $G(A) = G(D) = 1$, which establishes our claim. Thus, $G_0(A) = 1$. Now, by Lemma 1, we conclude that $p = 2$. Therefore, by Lemma 2, A can be written in the form $A = (a, E/F, -1)$. Since $-1 = 1$, by Theorem 14.7 of [6], we will obtain the contradiction $A \simeq M_s(F)$ and so the result follows. □

We shall need the following two lemmas to prove our next theorem.

Lemma 5. *Let D be an F-central division algebra of index p^e such that F contains a primitive p-th root of unity and D has no non-cyclic Galois splitting field of degree a power of p over F. Then we have:*

(i) *If $p = 2$, then either D has a cyclic splitting field E of degree 2^{te} for some integer t such that $-1 \in N_{E/F}(E^*)$ or D has a cyclic splitting field E such that E is the splitting field of a minimal polynomial of the form $x^{[E:F]} + 1$ and $F \subseteq E^{[E:F]}$.*

(ii) *If $p \neq 2$, then D has a cyclic splitting field of degree p^{te} for some positive integer t.*

Proof. Since F has a primitive p-th root of unity we have $(p, charF) = 1$. Set $L := F(\xi)$, where ξ is a primitive p^e-th root of unity and consider the L-algebra $D \otimes_F L$. By Theorem 17.1 of [2] which is a consequence of the Merkurjev-Suslin Theorem, $D \otimes_F L$ has an abelian splitting field of the form $K_0 := L(\sqrt[p^e]{a_1}, \ldots, \sqrt[p^e]{a_t})$, for some $a_i \in L$. View L as a maximal subfield in $M_m(F)$, where $m := [L : F]$. If $\sigma_i \in Gal(L/F)$, by Skolem-Noether Theorem, there is an element $A_i \in GL_m(F)$ such that $\sigma_i(x) = A_i x A_i^{-1}$ for all $x \in L$. Now, put $E := L(\sqrt[p^e]{A_i a_j {A_i^{-1}}_1} : 1 \leq j \leq t, 1 \leq i \leq m)$. Since $K_0 \subseteq E$, we conclude that E is a splitting field for D, and by Theorem 11.4 of [12], E/L is an abelian extension. We claim that $|Gal(E/F)| = [E : F]$, i.e., E/F is also a Galois extension. To see this, for each i we may extend σ_i to E by the rule $\bar{\sigma}_i(x) = A_i x A_i^{-1}$, for each $x \in E$, where A_i's and E may be viewed in $M_{[E:F]}(F)$. We first show that $\bar{\sigma}_i(E) \subseteq E$, which proves that $\bar{\sigma}_i$ is well defined. To see this, let α be a root of the polynomial $x^{p^e} - A_{i'} a_j A_{i'}^{-1}$ in $L[x]$. Then,

$\bar{\sigma_i}(\alpha) = A_i\alpha {A_i}^{-1}$ is also a root of $x^{p^e} - A_iA_{i'}a_jA_{i'}^{-1}A_i^{-1}$. Now, we have

$$A_iA_{i'}a_jA_{i'}^{-1}A_i^{-1} = \sigma_i\sigma_{i'}(a_j) = \sigma_k(a_j) = A_ka_jA_k^{-1},$$

for some $A_k \in GL_m(F)$. This shows that $\bar{\sigma_i}(\alpha) \in E$, and hence $\bar{\sigma_i} \in Aut(E)$. Now, set $G = \{\bar{\sigma_i}\tau_j : \sigma_i \in Gal(L/F), \tau_j \in Gal(E/L)\}$. It is clear that $\bar{\sigma_i}\tau_j \in Gal(E/F)$ for all i, j. We claim that $\mid G \mid= [E : F]$. To see this, if for some i, i', j, j' we have $\bar{\sigma_i}\tau_j = \bar{\sigma_{i'}}\tau_{j'}$, then $\bar{\sigma_i} \mid_L = \bar{\sigma_{i'}} \mid_L$ since $\tau_j \mid_L = \tau_{j'} \mid_L$. Hence, by Theorem 7.3 of [2], we obtain $A_iA_{i'}^{-1} \in Z_{M_m(F)}(L) = L$. Therefore, $\bar{\sigma_i} = \bar{\sigma_{i'}}$ and hence $\tau_j = \tau_{j'}$, i.e, every two elements of G are distinct, and so the claim is established. Thus, E/F is a Galois extension of degree a power of p which is also cyclic by our assumption. We now show that $F \subseteq E^{[E:F]}$. To see this, we first claim that $F \subseteq E^p$. If $b \in F \setminus E^p$, since F contains a primitive p-th root of unity, then $K = F(b^{1/p})$ is a cyclic extension of degree p such that $K \nsubseteq E$. Therefore, $E \otimes_F K$ is a non-cyclic Galois splitting field of degree a power of p over F that contradicts our assumption. So the claim is established. Now, consider the unique chain of all cyclic subfields in E: $E_0 = F \subset E_1 \subset E_2 \subset \cdots \subset E_k = E$. Because $F \subseteq E^p$, for each $x \in F$ there exists $y \in E$ such that $x = y^p$. From the uniqueness of the above chain we obtain $F(y) = E_1$ or $F(y) = F$. This implies that $F \subseteq E_1^p$. Again, consider the skew field component of the E_1-central simple algebra $D \otimes_F E_1$ with the same splitting field E. By taking $b \in E_1 \setminus E^p$ and using the same argument as above, we obtain $E_1 \subseteq E^p$ and hence $E_1 \subseteq E_2^p$. Therefore, the repeated use of the argument implies that $E_i \subseteq E_{i+1}^p$ and hence $F \subseteq E^{[E:F]}$, as required. Now, set $\Omega = \{\lambda \in F : \lambda^{p^r} = 1, r \in \mathbb{N}\}$. We have $\tau \in \Omega$, where τ is a primitive p-th root of unity. Hence, Ω is a nontrivial group. If Ω is an infinite group, then $\tau \in N_{E/F}(E)$. Hence, by repeated use of Exercise 15.3 in [2], E can be extended to a cyclic extension of degree p^{te} for some $t \in \mathbb{N}$ such that $\tau \in N_{E/F}(E)$ and the result follows. So assume that Ω is a finite cyclic group and consider $\zeta \neq 1$ as a generator of Ω. Since $F \subseteq E^{[E:F]}$, there exists $\eta \in E$ such that $\eta^{[E:F]} = \zeta$. If p^s is the minimum positive integer such that $\eta^{p^s[E:F]} = \zeta^{p^s} = \tau$, then η is a primitive $p^{s+1}[E : F]$-th root of unity. If not, we conclude that $\tau = 1$, a contradiction. Now, we prove that E is a splitting field of the minimal polynomial $x^{[E:F]} - \zeta$ over F. To see this, take $\eta_0 = \zeta$ and assume, by induction on i, that η_i, as a primitive p^{s+1+i}-th root of unity, be chosen such that $E_i = E_{i-1}(\eta_i)$. Since $E_i \subseteq E_{i+1}^p$, there exists $\eta_{i+1} \in E_{i+1}$ such that $\eta_{i+1}^p = \eta_i$. Hence, $E_{i+1} = E_i(\eta_{i+1})$, where η_{i+1} is a primitive p^{s+i+2}-th root of unity. Therefore, from our construction η, as a primitive $p^{s+1}[E : F]$-th root of unity, is not contained in E_{k-1}, i.e, $F(\eta) = E$. So, E is a splitting field of the minimal polynomial $x^{[E:F]} - \zeta$ over F. Now consider the following cases:

(i) If $p \neq 2$, then $N_{E/F}(\eta) = \zeta$ and hence $\tau \in N_{E/F}(E)$. By Exercise 15.3 in [2], E can be extended to a cyclic extension E' of degree $p[E : F]$. Now, by the repeated use of the construction above for E' in place of E and using the fact that D has no non-cyclic Galois splitting field of degree a power of p, we obtain a cyclic extension E of degree p^{te} for some integer t such that $F \subseteq E^{[E:F]}$.

(ii) If $p = 2$, suppose that $\zeta \neq -1$. Since $-\zeta = N_{E/F}(\eta)$ we have $-1 \in N_{E/F}(E)$, and this is reduced to the above case. But, if $\zeta = -1$, then we have a cyclic extension which is also the splitting field of the minimal polynomial $x^{[E:F]} + 1 = 0$, and also $F \subseteq E^{[E:F]}$.

□

Lemma 6. *Let G be a finite non-cyclic p-group. Then G has at least two distinct normal subgroups of index p.*

Proof. If G is an abelian group, then the conclusion is clear. So assume that $G \neq Z(G)$ and consider the group $G/Z(G)$. From group theory we know that $G/Z(G)$ is also a non-cyclic p-group. Now, use induction on the order of G to obtain the result. □

Now, we are able to prove the following interesting result.

Theorem 3. *Let D be an F-central division algebra of index p^e such that F contains a primitive p-th root of unity and $G(D) = 1$. Then D is a quaternion algebra.*

Proof. First assume that D has a non-cyclic Galois splitting field E of degree a power of p. Since $G(D) = 1$, by corollary 4.19 of [10], we have $N(D^*) = RN(D^*)$, i.e., $F^{*p^e} = F^{*p^{2e}}$. By Lemma 6, $G := Gal(E/F)$ has at least 2 distinct normal subgroups H_1, H_2 of index p in G. If M_1, M_2 are the fixed fields of H_1, H_2 in E , respectively, then from Galois theory both M_1, M_2 are cyclic extensions of degree p in E over F. Therefore, by Hilbert's "Satz90", for $i = 1, 2$ there is $b_i \in M_i$ such that $b_i^{-1}\sigma_i(b_i) = \tau$, where $Gal(M_i/F) =< \sigma_i >$, and τ here is a primitive p-th root of unity in F. From the relation $F^{*p^e} = F^{*p^{2e}}$, since $b_i^p \in F^*$, there are also $c_1, c_2 \in F^*$ such that $(b_i^p)^{p^e} = c_i^{p^{2e}}$, and hence $(b_i^p(c_i^{-1})^{p^e})^{p^e} = 1$. Let Ω denote the group of p^e-th roots of unity in F. Since $b_i \notin F$, then $b_i^p(c_i^{-1})^{p^e}$ for $i = 1, 2$ are generators of Ω. But, this is not possible since $M_1 \neq M_2$, and both M_1, M_2 lie in E. Thus, we may assume that D has no non-cyclic Galois splitting field of degree a power of p. Now, by Lemma 5, we consider two following cases:

(i) If $p \neq 2$, by Lemma 5, D has a cyclic splitting field E of degree p^{te} for some integer t. From the proof of Theorem 2 with $m = p^{(t-1)e}$, E can be embedded in the cyclic algebra $A = M_m(D)$ as a maximal subfield such that $G(A) = 1$. But, by Lemma 1, we obtain $M_m(D) = M_r(F)$ for some $r \in \mathbb{N}$, which is not possible.

(ii) If $p = 2$, by Lemma 5, suppose that D has a cyclic splitting field E of degree 2^{te} such that $-1 \in N_{E/F}(E)$, then the cyclic algebra defined in (i), by Lemma 2, can be written in the form $M_m(D) = \oplus_{i=0}^{[E:F]-1} Ea^i$ such that $a^{[E:F]} = -1$. But, $-1 \in N_{E/F}(E)$. Therefore, by the proof of Lemma 14.7 of [6], we obtain $M_m(D) = M_r(F)$ for some $r \in \mathbb{N}$, that contradicts our assumption. So, D has a cyclic splitting field E in which the minimal polynomial $x^{[E:F]} + 1$ splits. If η is an element in E such that its minimal polynomial over F is $x^{[E:F]} + 1$, then $-\eta^{2^k} = N_{E/F}(\eta) = 1$, where $[E : F] = 2^k$. On the other hand, since $1 + N_{E/F}(\eta) = N_{E/F}(\eta + 1) = RN_{M_m(D)/F}(\eta + 1) \in F^{2^k}$, it follows that $\sqrt{2} \in F$. Thus, if $k > 1$, then $\eta^{2^k} + 1 = (\eta^{2^{k-1}} + 1)^2 - 2\eta^{2^{k-1}}$ can be decomposed further which leads to a contradiction that the minimal polynomial of η has degree less than $[E : F]$. Therefore, we have $k = 1$ which means that D is a quaternion algebra.

□

Finally, we shall need the following lemmas to prove our last result.

Lemma 7. *Let D be an F-central division algebra of index $p_1^{e_1} \cdots p_k^{e_k}$. Suppose that $D = D_1 \otimes_F \ldots \otimes_F D_k$ is the primary decomposition of D with $i(D_i) = p_i^{e_i}$. If $G(D) = 1$, then $G(D_i) = 1$ for all $1 \leq i \leq k$.*

Proof. It is enough to prove the result for the case $D = A \otimes_F B$, where A, B are two division algebras such that $(i(A), i(B)) = 1$ and also $G(A \otimes_F B) = 1$. Consider the following embeddings:

$$A \xrightarrow{i} A \otimes_F B \xrightarrow{i_1} A \otimes_F B \otimes_F B^{op} \xrightarrow{i_2} A \otimes_F M_m(F) \xrightarrow{j} M_m(A),$$

where $m = i(B)$, and set $\varphi = j \circ i_2 \circ i_1$. Thanks to Dieudonne determinent, we then obtain the following homomorphisms

$$A \rightarrow \frac{A \otimes_F B}{(A \otimes_F B)'} \overset{det \circ \varphi}{\rightarrow} \frac{A}{RN_{A/F}(A^*)A'} = G(A).$$

By Corollary 2.4 of [3], since the exponent of $G(A)$ divides $i(A)$ and $(i(A), i(B)) = 1$, we conclude that the image of A under $det \circ \varphi$ is

$G(A)$. Now, we claim that for each $y \in RN_{A\otimes_F B/F}(A \otimes_F B)$, we have $det \circ \varphi(y) = 1$. By the Reduced Tower formula [2], for each $x \in A \otimes_F B$ we have

$$RN_{A/F}(det(x)) = RN_{M_m(A)/F}(x) = RN_{A\otimes_F B/F}(x)^m.$$

If $y = RN_{A\otimes_F B/F}(x) \in F$, then

$$det\circ\varphi(y) = det\circ\varphi(RN_{A\otimes_F B/F}(x)) = RN_{A\otimes_F B/F}(x)^m = RN_{A/F}(det(x)),$$

i.e, the image of $det \circ \varphi(y)$ in $G(A)$ is identity, and so the claim is established. Hence, we obtain the following embeddings

$$A \rightarrow G(A \otimes_F B) \overset{det\circ\varphi}{\rightarrow} G(A).$$

Therefore, since the domain of $\det \circ\varphi$ is identity, and also $det \circ \varphi$ is surjective, we obtain $G(A) = 1$, and similarly $G(B) = 1$. □

Proposition 1. *Let D be an F-central division algebra of index $p_1^{e_1} \cdots p_k^{e_k}$. If either of the following conditions holds, then we have $G(D) \neq 1$.*

(i) *One of the primary components of D is a p_i-algebra.*
(ii) *F contains a primitive p_i-th root of unity for at least one i, and none of the primary components of D is a quaternion algebra.*

Proof. Assume on the contrary that $G(D) = 1$. If D_i is an i-th primary component of D that satisfies (i) or (ii), then by Lemma 7, we have $G(D_i) = 1$. By Theorem 2, D_i is not a p_i-algebra, i.e., D_i does not satisfy (i). Therefore, by Theorem 3, we conclude that D_i is a quaternion division algebra which contradicts our assumption. □

Corollary 1. *Let D be an F-central division algebra that satisfies the conditions of Proposition 1. Then D^* has a maximal subgroup.*

Proof. Since $G(D) \neq 1$ the result follows. □

Corollary 2. *Let D be an F-central division algebra of index p^e such that D is not a quaternion algebra. Then D^* has a maximal subgroup if either of the following conditions holds.*

(i) *F has characteristic zero.*
(ii) *F has characteristic p.*
(iii) *F has a primitive p-th root of unity.*

Proof. (i) Assume that F has characteristic zero. If $G(D) \neq 1$, then the result follows. So, assume that $G(D) = 1$. If $Z(D') \neq 1$, then D' contains a primitive p-th root of unity. Therefore, the proof is reduced to (iii). But, when $Z(D') = 1$ we have $D^* = F^* \times D'$. Hence, by Theorem 6 of [1], F^* has a normal maximal subgroup. So, D^* has also a normal maximal subgroup.

(ii) If F has characteristic p, then by Theorem 2, we have $G(D) \neq 1$ and so the result follows.

(iii) Assume that F has a primitive p-th root of unity. If $G(D) \neq 1$, the result follows. So, assume that $G(D) = 1$. By Theorem 3, D is a quaternion algebra that is a contradiction.

□

Acknowledgment. The authors thank the Research Council of Sharif University of Technology for support.

References

[1] S .Akbari, M. Mahdavi-Hezavehi, *On the Existence of Normal Maximal Subgroups in Division Rings*. J. Pure Appl. Algebra 171(2-3)(2002), 123-131.

[2] P. K. Draxl, Skew Fields, London Math. Soc. Lecture Notes Series. Vol 81, Cambridge, Univ. Press Cambridge(1983).

[3] R. Hazrat, *SK_1-like Functors for Division Algebras*, J. of. Algebra 239(2001), 573-588.

[4] R. Hazrat, M. Mahdavi-Hezavehi, B. Mirzaii, *Reduced K-Theory and the Group $G(D) = D^*/F^*D'$*, Algebraic K-theory and its applications (Trieste, 1997), 403-409.

[5] N. Jacobson, Finite Dimensional Division Algebras Over Fields, Berlin/Heidelberg : Springer,(1996).

[6] T.Y.Lam, A First Course in Noncommutative Rings, GTM, No.131, Springer-Verlag, (1991).

[7] M. Mahdavi-Hezavehi, *Tits Alternative for Maximal Subgroups of $GL_n(D)$*, J. of Algeb., 271(2004), 518-528.

[8] M. Mahdavi-Hezavehi, *Commutator Subgroups of Finite Dimensional Division Algebras*, Rev. Roumaine Math. Pure Appl. 43(1998) (9-10), 853-867.

[9] M. Mahdavi-Hezavehi, *Free Subgroups in Maximal Subgroups of $GL_1(D)$*, J. Algeb., 241(2001) 720-730.

[10] M. Mahdavi-Hezavehi, *Determinant-like Functions for Matrices over Finite Dimensional Divsion Algebras*, Proc. of the Symposium on Algebraic K-Theory, Trieste 1997, World Scientific Pub., (1999).

[11] M. Mahdavi-Hezavehi, *Extending Valuations to Algebraic Division Algebras*, Comm. Algebra 22 (1994), no. 11, 4373-4378.

[12] P. Morandi, Fields and Galois Theory, New York, Springer (1996).

[13] R. Pierce, Associative Algebra, Springer-Verlag, New York, Heidelberg Berlin (1982).

[14] D. J. S. Robinson, A Course in the Theory of Groups, Graduate Text in Mathematics, No. 80, Springer-Verlag, (1982).

Department of Mathematical Sciences, Sharif University of Technology, P. O. Box 11365-9415. Tehran, Iran
E-mail address: keshavarzi_pour@mehr.sharif.edu &, mahdavih@sharif.edu